UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,851	05/22/2001	Ralph S. Hoefelmeyer	COS 00 017	8371

25537 7590 07/13/2005

MCI, INC
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/862,851	HOEFELMEYER ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 are pending in the Application.

Response to Arguments

2. Applicant's arguments filed 4/28/2005, with respect to the rejection(s)of claim(s) 1-32 under U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. **Claims 1, 5-7, 9, 13-15, 17-23, 25-26, 28-29 and 31-32** are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Ji et al. (US Pat. No. 5,623,600, hereinafter "Ji") and Xu, US Patent Pub. No. 2002/0032766 and further in view of U.S. Pat. No. 6,385,747 to Scott et al. (hereinafter "Scott ").

As per claims 1 and 9, Ji teaches a method /system for malicious code detection (abstract), comprising:

A plurality of scanning computer systems configured for scanning content for malicious code and generating an alarm when the content contains malicious code (Figure 3 and related text, col. 4, lines 63-65, routines for detecting viruses in file transfers and messages (i.e. a plurality of computer scanning systems), col. 7, lines 65-67, output of virus checking is echoed to the client task (i.e. generating an alarm)) ; and

a front-end processor, coupled to a scanning computer system, configured for receiving a flow of content from an external network and distributing a copy of the flow to each of the scanning computer systems for scanning (Figure 1 and related text, col. 3, lines 51-63, gateway node 33 (front-end processor) performs virus detection for all files through FTP proxy being transmitted into or out of a network and also performs virus detection on all messages through SMTP Proxy server being transmitted into or out of an associated network, see also Figure 3 and related text, col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40), and

a detection management system, coupled to the scanning computer system, configured for employing a countermeasure on the flow if the scanning computer system generates the alarm (col. 11, lines 3-40, i.e. Ji's proxy servers respond in variety of ways (i.e. a countermeasure

taken) according to user's needs specified in a configuration file, see also col. 11, lines 3-40, and that an action is taken based on configuration settings).

Ji fails to teach distributing a common copy of the flow to each of the scanning computer systems in parallel for scanning.

However, Xu discloses a plurality of scanning computer systems and distributing a common copy of the flow to each of the scanning computer systems for scanning, Xu, page 18, paragraphs 228 (Xu).

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems of Xu for scanning a common copy of the flow because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

It is noted that the combination of Ji and Xu fails to disclose (as Applicant persuasively argued) distributing a common copy of the flow to each of the scanning computer systems in parallel for scanning.

However, Scott teaches a technique for broadcasting (i.e. distributing) the same test inputs (common copy of the flow), in parallel, used in testing (scanning) to each of the replicated components of an electronic device under test (Scott, abstract).

Therefore, it would have been further obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Scott's parallel scanning systems within the system of Ji and Xu as combined above, in order to speed up the scanning process as suggested by Scott, col. 2, lines 63-67.

As per claims 5, 13 and 31-32, Ji does not teach but Xu teaches the system and method according to claims 1 and 9 respectively, wherein scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code, Xu, page 18, paragraphs 228 (Xu).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Xu within the system of Ji to incorporate virus scanning software differ in their capabilities as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228.

As per claims 6 and 14, Ji teaches the system and method according to claims 1 and 9 respectively, wherein the flow includes at least one of a hypertext markup file and a transferred file [col. 5, lines 28-38].

As per claims 7 and 15, Ji teaches the system/method according to claims 1 and 9 respectively, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code (col. 11, lines 3-40, i.e. Ji's proxy servers respond in variety of ways (i.e. a countermeasure taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory (i.e. quarantining and blocking the flow) on the proxy server and notify (i.e. informing the recipient) the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking

program into the mail message in place of encoded portions and sending the mail message. The teaching of Ji suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined).

As per claims 18 and 17, Ji teaches a method and a front-end system (Figure 1 and related text, col. 3, lines 51-63, gateway node 33 performs virus detection foe all files (through FTP proxy) being transmitted into or out of a network and also performs virus detection on all messages through SMTP Proxy server (i.e. a plurality of scanning computer systems) being transmitted into or out of an associated network, see also Figure 4 and related text, col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40), coupled to an external network and a plurality of scanning computer systems, said front-end system comprising one or more processors (Figure 2, CPU 42), a communications interface (communication unit 54), and a computer-readable medium (Figure 3 and related text, col. 4, lines 56-67, memory 44 comprises a routine for detecting viruses) bearing instructions for causing the one or more processors upon execution thereof to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file [Figure 3 and related text, col. 4, line 66, the FTP proxy server 60 and SMTP proxy server 62 controls files and messages to and from the gateway node 33, see also col. 5, lines 28-38];

Ji does not teach but Xu teaches duplicating the flow to produce a plurality of common copies of the flow; and

distributing the common copies of the flow to each of the scanning computer systems, Xu, page 18, paragraphs 228 (Xu).

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems of Xu for scanning a common copy of the flow because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

It is noted that the combination of Ji and Xu fails to disclose (as Applicant persuasively argued) distributing a common copy of the flow to each of the scanning computer systems in parallel.

However, Scott teaches a technique for broadcasting (i.e. distributing) the same test inputs (common copy of the flow) used in testing (scanning) to each of the replicated components of an electronic device under test, Scott, abstract.

Therefore, it would have been further obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Scott's parallel scanning systems within the system of Ji and Xu as combined above, in order to speed up the scanning process as suggested by Scott, col. 2, lines 63-67.

Claim 19 recites a storage medium having instructions to execute the method of claim 18, therefore the same rejection applies.

As per claims 20 and 21, JI teaches a malicious code detection cluster and a method of detecting malicious code in an internal network, comprising:

an internal network coupled to a front-end processor (Figure 3 and related text, gateway node 33) and a detection management system (col. 4, lines 63-65 disclose routines for detecting

viruses in file transfers and messages which include the FTP proxy server 60 and the SMTP proxy server 62);

a plurality of scanning computer systems coupled to the internal network and configured for (col. 4, line 66, the FTP proxy server 60 and SMTP proxy server 62 controls files and messages to and from the gateway node 33, see also col. 5, lines 28-38):

While Ji discloses receiving a flow of content from the front-end processor , said flow including at least one of a hypertext markup file and a transferred file (Figure 3 and related text, col. 4, line 66, the FTP proxy server 60 and SMTP proxy server 62 controls files and messages to and from the gateway node 33, see also col. 5, lines 28-38] and executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the flow (col. 4, lines 56-65 discloses memory 44 comprising FTP proxy server and SMTP proxy server and routines for detecting viruses in file transfers and messages (i.e. having different, corresponding coverage of malicious code)); and

transmitting an alarm to the detection management system when the flow contains malicious code as detected by at least one of the anti-virus scanning software (col. 7, lines 65-67).

Ji is silent in disclosing receiving respective common copies of a flow in parallel and scan the common copies of the flow in parallel.

However, Xu discloses a plurality of scanning computer systems and distributing a common copy of the flow to each of the scanning computer systems for scanning, Xu, page 18, paragraphs 228 (Xu).

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems of Xu for scanning a common copy of the flow because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

It is noted that the combination of Ji and Xu fails to disclose (as Applicant persuasively argued) receiving respective common copies of a flow in parallel and scan the common copies of the flow in parallel.

However, Scott teaches a technique for broadcasting (i.e. distributing) the same test inputs (common copy of the flow) used in testing (scanning) to each of the replicated components of an electronic device under test, Scott, abstract.

Therefore, it would have been further obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Scott's parallel scanning systems within the system of Ji and Xu as combined above, in order to speed up the scanning process as suggested by Scott, col. 2, lines 63-67.

As per claims 22-23, 28-29, 25-26 and 28-29, Ji teaches a method of managing malicious code detection, a computer –readable medium bearing instructions for managing malicious code detection and a detection management system (gateway node 33), coupled to a plurality of scanning computer systems (Figure 3 and related text, col. 4, line 66, the FTP proxy server 60 and SMTP proxy server 62 controls files and messages to and from the gateway node 33, see also col. 5, lines 28-38), said detection management system comprising one or more processors (FTP proxy server 60 and SMTP proxy server 62), a communications interface (communication unit 54), and a computer-readable medium bearing instructions arranged for

causing the one or more processors upon execution (col. 4, lines 63-65 disclose routines for detecting viruses in file transfers and messages which include the FTP proxy server 60 and the SMTP proxy server 62) thereof to perform the steps of:

receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems contains malicious code (col. 7, lines 65-67), said flow including at least one of a hypertext markup file and a transferred file (col. 4, lines 32-33); and

employing a countermeasure on the common flow if at least one of the scanning computer systems generates an alarm on a piece of the malicious code, wherein said employing the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code [col. 7, lines 65-67 discloses that an output of the virus checking program is echoed to the client task by the FTP proxy server (i.e. an alarm on a piece of malicious code, and col. 11, lines 3-40 discloses that proxy servers respond in variety of ways (i.e. a countermeasure taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory (i.e. quarantining and blocking the flow) on the proxy server and notify (i.e. informing the recipient) the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching

of Ji suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined].

JI is silent in disclosing a common flow of the content scanned by the scanning computer systems in parallel and employing a countermeasure on the common flow.

However, Xu discloses a plurality of scanning computer systems and distributing a common copy of the flow to each of the scanning computer systems for scanning, Xu, page 18, paragraphs 228 (Xu).

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems of Xu for scanning a common copy of the flow because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

It is noted that the combination of Ji and Xu fails to disclose (as Applicant persuasively argued) a common flow of the content scanned by the scanning computer systems in parallel and employing a countermeasure on the common flow.

However, Scott teaches a technique for broadcasting (i.e. distributing) the same test inputs (common copy of the flow) used in testing (scanning) to each of the replicated components of an electronic device under test, Scott, abstract.

Therefore, it would have been further obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Scott's parallel scanning systems within the system of Ji and Xu as combined above, in order to speed up the scanning process as suggested by Scott, col. 2, lines 63-67.

4. **Claims 8 and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, USP 5,623,600 to Ji et al. (hereinafter "Ji"), US Patent Pub. No. 2002/0032766 to Xu and USP 6,385,747 to Scott et al. (hereinafter "Scott ") and further in view of prior art of record, USP 6,338,141 to Wells.

As per claims 8 and 16, Ji teaches a system and a method for malicious code detection, comprising:

A remote site detection system (Figure 3 and related text, gateway node 33 with routines for detecting viruses, col. 4, lines 63-66) configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat (col. 7, lines 60-63);

a front-end processor (Figure 3 and associated text, gateway node 33), coupled to the scanning computer systems (Figure 3, col. 4, lines 63-66, the FTP proxy server 60 and SMTP proxy server 62 controls files and messages to and from the gateway node 33, see also col. 5, lines 28-38), said detection management system comprising one or more processors (col. 4, lines 63-66, routines for detecting viruses in file transfers and messages which include FTP proxy server 60 and SMTP proxy server 62), configured for receiving a flow of content from an external network and distributing (col. 3, lines 4-16) the flow to each of the scanning computer systems for scanning, said flow including at least one of a hypertext markup file and a transferred file [col. 5, lines col. 5, lines 33-36, see also col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40]; and

employing a countermeasure on the flow if at least one of the scanning computer systems generates an alarm on the piece of malicious code, said countermeasure including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow

of the malicious code and generating an alarm when the content contains malicious code [col. 7, lines 65-67 discloses that an output of the virus checking program is echoed to the client task by the FTP proxy server (i.e. an alarm on a piece of malicious code), and col. 11, lines 3-40 discloses that proxy servers respond in variety of ways (i.e. a countermeasure taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory (i.e. quarantining and blocking the flow) on the proxy server and notify (i.e. informing the recipient) the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching of Ji suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention takes actions (countermeasures) on the flow if an encoded portion is determined]

Ji does not disclose but Xu discloses a plurality of scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code for scanning content for malicious code, Xu, page 18, paragraphs 228).

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems of Xu for scanning a common copy of the flow because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

It is noted that the combination of Ji and Xu fails to disclose (as Applicant persuasively argued) a common flow of the content scanned by the scanning computer systems in parallel and employing a countermeasure on the common flow.

However, Scott teaches a technique for broadcasting (i.e. distributing) the same test inputs (common copy of the flow) used in testing (scanning) to each of the replicated components of an electronic device under test, Scott, abstract.

Therefore, it would have been further obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Scott's parallel scanning systems within the system of Ji and Xu as combined above, in order to speed up the scanning process as suggested by Scott, col. 2, lines 63-67.

Xu discloses that at least one of the scanning computer systems generates an alarm on the piece of the malicious code (col. 7, lines 65-67), but Ji-Xu combination fails to teach a detection management system, coupled to the scanning computer systems, configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computer systems generates an alarm on the piece of malicious code; and

causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files,

as they are checked for viruses, are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

Therefore, It would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Ji as modified to provide a virus detection system with high degree of certainty and to avoid false identification while recognizing new variants of known viruses, Wells, col.2, lines 22-46.

5. Claims 2-4, 10-12, 24, 27 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji, Xu and Scott and further in view of prior art of record, USP 6,338,141 to Wells.

As per claims 2-4, 10-12, Ji as modified fails to teach a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer system,

a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat,

wherein the detection management system is further configured for causing the signatures stored at the remote detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files, as they are checked for viruses, are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

It would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Ji to provide a virus detection system with high degree of certainty and to avoid false identification while recognizing new variants of known viruses, Wells, col. 2, lines 22-46.

As per claims 24, 27 and 30, While Ji teaches at least one of the scanning computer systems generate an alarm on the piece of malicious code (col. 7, lines 65-67) but Ji as modified fails to disclose the detection management system, the method and the computer –readable according to claims 22, 25 and 28 respectively, wherein the detection management system is further coupled to a remote site detection system and said instructions are further arranged for causing the one or more processors to perform the steps of:

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems in the flow when at least one of the scanning computer systems generates an alarm on the piece of malicious code; and

causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files, as they are checked for viruses, are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

Therefore, it would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Ji as modified to provide a virus detection system with high degree of certainty and to avoid false identification while recognizing new variants of known viruses, Wells, col. 2, lines 22-46.

Conclusion

6. USP 6, 574,737 to Kingsford et al. is a computer network penetration test discovers vulnerabilities in the network using a number of scan modules. The scan modules perform their scanning of the network separately but in parallel. A scan engine controller oversees the data fed to and received from the scan modules, and controls the sharing of information among the modules according to data records and configuration files that specify how a user-selected set of

penetration objectives should be carried out. The system allows for penetration strategies to be attempted simultaneously and independently.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
7/6/05